

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Shinichi YASUDA, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: RANDOM NUMBER GENERATOR

**REQUEST FOR PRIORITY**

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number \_\_\_\_\_, filed \_\_\_\_\_, is claimed pursuant to the provisions of **35 U.S.C. §120**.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**:  
Application No. \_\_\_\_\_ Date Filed \_\_\_\_\_
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY  
Japan

APPLICATION NUMBER  
2002-269129

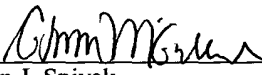
MONTH/DAY/YEAR  
September 13, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_
- ☐ were submitted to the International Bureau in PCT Application Number \_\_\_\_\_  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. \_\_\_\_\_ filed \_\_\_\_\_; and
- ☐ (B) Application Serial No.(s) \_\_\_\_\_  
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
Marvin J. Spivak

Registration No. 24,913  
C. Irvin McClelland  
Registration Number 21,124

Customer Number

**22850**

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月13日

出 願 番 号

Application Number:

特願2002-269129

[ ST.10/C ]:

[ JP2002-269129 ]

出 願 人

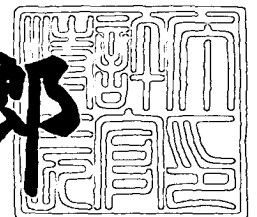
Applicant(s):

株式会社東芝

2003年 4月 4日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3023464

【書類名】 特許願

【整理番号】 13B026001

【提出日】 平成14年 9月13日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/58

【発明の名称】 乱数生成回路

【請求項の数】 8

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
    研究開発センター内

    【氏名】 安田 心一

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
    研究開発センター内

    【氏名】 藤田 忍

【特許出願人】

    【識別番号】 000003078

    【氏名又は名称】 株式会社 東芝

【代理人】

    【識別番号】 100083806

    【弁理士】

    【氏名又は名称】 三好 秀和

    【電話番号】 03-3504-3075

【選任した代理人】

    【識別番号】 100068342

    【弁理士】

    【氏名又は名称】 三好 保男

【選任した代理人】

    【識別番号】 100100712

【弁理士】

【氏名又は名称】 岩▲崎▼ 幸邦

【選任した代理人】

【識別番号】 100100929

【弁理士】

【氏名又は名称】 川又 澄雄

【選任した代理人】

【識別番号】 100108707

【弁理士】

【氏名又は名称】 中村 友之

【選任した代理人】

【識別番号】 100095500

【弁理士】

【氏名又は名称】 伊藤 正和

【選任した代理人】

【識別番号】 100101247

【弁理士】

【氏名又は名称】 高橋 俊一

【選任した代理人】

【識別番号】 100098327

【弁理士】

【氏名又は名称】 高松 俊雄

【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【その他】

国等の委託研究の成果に係る特許出願（平成14年度通信・放送機構「高度情報セキュリティに向けた真性乱数生成用集積回路の研究開発」委託研究、産業活力再生特別措置法第30条の適用を受けるもの）

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数生成回路

【特許請求の範囲】

【請求項 1】 クロック信号をクロック入力端子に入力し、ランダム信号をカウントイネーブル端子に入力し、前記ランダム信号の変化に応じて前記クロック信号のカウント値を出力するカウンタ回路と、

前記ランダム信号の変化に応じて前記カウント値をラッチし第 1 の乱数信号を出力する第 1 のラッチ回路

とを備えることを特徴とする乱数生成回路。

【請求項 2】 前記ランダム信号は、周波数の増加に対してパワースペクトルが減少する特性を有することを特徴とする請求項 1 に記載の乱数生成回路。

【請求項 3】 周期が一定の乱数取得クロック信号と前記第 1 の乱数信号とを入力し、前記乱数取得クロック信号の変化に応じて前記第 1 の乱数信号をラッチし、第 2 の乱数信号を出力する第 2 のラッチ回路を更に備えることを特徴とする請求項 1 に記載の乱数生成回路。

【請求項 4】 パルスカウンタを前記カウントイネーブル端子に接続し、前記パルスカウンタの出力を前記ランダム信号とすることを特徴とする請求項 1 に記載の乱数生成回路。

【請求項 5】 ランダム信号を第 1 の入力端子に、クロック信号を第 2 の入力端子に入力し、前記ランダム信号と前記クロック信号の論理積を出力するアンド回路と、

前記論理積出力に応じてハイレベルとローレベルを交互に出力する分周ラッチ回路と、

前記ランダム信号の変化に応じて前記カウント値をラッチし乱数信号を出力する第 1 のラッチ回路

とを備えることを特徴とする乱数生成回路。

【請求項 6】 前記ランダム信号は、周波数の増加に対してパワースペクトルが減少する特性を有することを特徴とする請求項 5 に記載の乱数生成回路。

【請求項 7】 周期が一定の乱数取得クロック信号と前記第 1 の乱数信号と

を入力し、前記乱数取得クロック信号の変化に応じて前記第 1 の乱数信号をラッチし、第 2 の乱数信号を出力する第 2 のラッチ回路を更に備えることを特徴とする請求項 5 に記載の乱数生成回路。

【請求項 8】 パルスカウンタを前記カウントイネーブル端子に接続し、前記パルスカウンタの出力を前記ランダム信号とすることを特徴とする請求項 5 に記載の乱数生成回路。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、乱数生成回路に係り、特に規則性のない乱数を生成する乱数生成回路に関する。

【 0 0 0 2 】

【従来の技術】

従来より、乱数による暗号化は、電子商取引や、無線通信等の情報通信において、パスワードの生成、暗号鍵生成、ID 情報の生成、及びデジタル署名付加情報の生成等の情報の保護に用いられる。乱数の生成方法は、ソフトウェアによって発生させる方法が広く採用されている。しかし、ソフトウェアによる乱数生成方法は、プログラムに記載された数式に基づいて乱数を生成するため、何らかの規則性を有するという欠点がある。すなわち、規則性を有する暗号化は解読されてしまう可能性があり、個人情報の十分な保護が図れない問題があった。すなわち、周波数特性に依存しない乱数が求められていた。

【 0 0 0 3 】

これに対し、 $1/f$  特性を有する雑音発生源から発生される雑音に基づいて、 $1/f$  特性による周期性を持たない乱数を乱数生成回路により生成する方法がある（特許文献 1 参照。）。

【 0 0 0 4 】

特許文献 1 に記載の乱数生成回路は、図 1 6 に示すように、雑音発生回路 2 0 1、2 0 2 と、雑音発生回路 2 0 1、2 0 2 の出力側にそれぞれ接続された差動回路 2 0 3 と、差動回路 2 0 3 の出力側に接続された A/D 変換回路 2 0 4 と、

A/D変換回路204の出力側に接続された演算回路205とにより構成される。

#### 【0005】

先ず、雑音発生回路201、202は $1/f$ 特性を有する雑音信号を出力する。次に、差動回路203は、雑音発生回路201、202から出力される2つの雑音信号の差動信号をアナログ信号として出力する。A/D変換回路204は、差動回路から出力されるアナログ信号をデジタル信号に変換する。演算回路205は、デジタル変換された信号がスレッシュホールドレベルに達しない場合には「0」を出力し、スレッシュホールドレベルに達する場合には「1」を出力する。演算回路205は「0」と「1」の出現する確率が0.5になるようにスレッシュホールドレベルを調節していた。

#### 【0006】

##### 【特許文献1】

特開2002-41281号公報

#### 【0007】

##### 【発明が解決しようとする課題】

しかし、図16に示す乱数生成回路はフィルタ、差動回路等のアナログ回路と、2つの雑音発生回路を用いるため、専有面積が大きくなる問題があった。更に、「0」と「1」の出現する確率を演算回路205のスレッシュホールドレベルを変更し設定する必要がある。

#### 【0008】

本発明の目的は、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供することである。

#### 【0009】

##### 【課題を解決するための手段】

上記目的を達成するために、本発明の第1の特徴は、クロック信号をクロック入力端子に入力し、ランダム信号をカウントイネーブル端子に入力し、ランダム信号の変化に応じてクロック信号のカウント値を出力するカウンタ回路と、ラン



ダム信号の変化に応じてカウント値をラッチし第 1 の乱数信号を出力する第 1 のラッチ回路とを備えることを要旨とする。

#### 【0 0 1 0】

本発明の第 1 の特徴によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供できる。

#### 【0 0 1 1】

上記目的を達成するために、本発明の第 2 の特徴は、ランダム信号とクロック信号を入力し、ランダム信号及びクロック信号の論理積出力に応じてハイレベルとローレベルを交互に出力する分周回路と、ランダム信号の変化に応じてカウント値をラッチし乱数信号を出力するラッチ回路とを備えることを要旨とする。

#### 【0 0 1 2】

本発明の第 2 の特徴によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供できる。

#### 【0 0 1 3】

#### 【発明の実施の形態】

次に、図面を参照して本発明の第 1 ～第 5 の実施の形態を説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

#### 【0 0 1 4】

まず、第 1 ～第 5 の実施の形態で用いられる「ランダム信号 R S」について説明する。「ランダム信号 R S」とは、オン幅とオフ幅の時間が一定でない複数の矩形波からなるデジタル信号である。また、「ランダム信号 R S」は、周波数の増加に対してパワースペクトルが減少する特性を有する。矩形波の振幅は、一定であることが望ましいがここでは特に限定されない。例えば、ランダム信号 R S は、抵抗とコンデンサにより構成される C R 遅延回路の遅延時間を利用した発振回路により生成される。抵抗やコンデンサの値がランダムに揺らぐことを利用して生成される。パワースペクトルが減少する信号の例としては、 $1/f$  特性を有す

る揺らぎ信号等が挙げられる。「 $1/f$ 」とは、フーリエ分析したパワースペクトルがフーリエ周波数  $f$  に反比例して 4 5 度の傾斜を持つものをいう。すなわち、配列、空間等の時系列データのスペクトル解析を行なうと、その両対数プロットで得られる傾きが  $-1$  を示す。

## 【 0 0 1 5 】

## (第 1 の実施の形態)

本発明の第 1 の実施の形態に係る乱数生成回路 1 0 a は、図 1 に示すように、クロック信号  $CS$  をクロック入力端子  $CK$  に入力し、ランダム信号  $RS$  をカウンタイネーブル端子  $CE$  に入力し、ランダム信号  $RS$  の変化に応じてクロック信号  $CS$  のカウント値を出力するカウンタ回路 1 と、ランダム信号  $RS$  の変化に応じてカウント値をラッチし乱数信号  $RNS$  を出力する第 1 のラッチ回路 3 とを備える。更に、インバータ 2 が矩形波入力端子 5 1 及びカウンタ回路 1 のカウンタイネーブル端子  $CE$  との接続点と、第 1 のラッチ回路 3 のクロック入力端子  $CK$  との間に接続される。矩形波入力端子 5 1 は、カウンタ回路 1 のカウンタイネーブル端子  $CE$  にランダム信号  $RS$  を入力する端子である。クロック入力端子 5 2 は、カウンタ回路 1 のクロック入力端子  $CK$  に電氣的に接続されたクロック信号  $CS$  を入力する端子である。インバータ 2 の出力端子は、第 1 のラッチ回路 3 のクロック入力端子  $CK$  に電氣的に接続される。カウンタ回路 1 の出力端子  $Q$  は、第 1 のラッチ回路 3 の入力端子  $D$  に電氣的に接続される。第 1 のラッチ回路 3 の出力端子  $Q$  は、乱数出力端子 5 3 に電氣的に接続される。

## 【 0 0 1 6 】

本発明の第 1 の実施の形態に係る乱数生成回路 1 0 a の動作を、図 2 を用いて説明する。

## 【 0 0 1 7 】

(イ) 先ず、時刻  $t_1$  において、図 2 (a) に示すように、矩形波入力端子 5 1 に入力されるランダム信号  $RS$  がローレベルからハイレベルとなる。

## 【 0 0 1 8 】

(ロ) 時刻  $t_1$  から  $t_2$  までの間、ランダム信号  $RS$  がハイレベルの状態では、カウンタ回路 1 は、出力端子  $Q$  からカウント信号  $CTS$  を出力する。図 2 (c

）に示すように、カウント信号 C T S は、図 2（b）に示すクロック信号 C S の立ち上がりエッジ検出毎にハイレベルとローレベルを交互に切り換える。ここでは、カウンタ回路 1 は、例示的に 1 カウントごとにローレベルとハイレベルが交互に切り換わる 1 ビットカウンタであるとする。

## 【 0 0 1 9 】

（ハ）時刻  $t_2$  において、ランダム信号 R S がハイレベルからローレベルとなる。ランダム信号 R S がローレベルとなると、インバータ 2 は、図 2（d）に示すように、ハイレベルとなるランダム反転信号 R S バーを出力する。ランダム反転信号 R S バーがハイレベルとなると、第 1 のラッチ回路 3 は、クロック入力端子 C K の立ち上がりエッジでカウンタ回路 1 から出力されるカウント信号 C T S をラッチし、図 2（e）に示すように、乱数信号 R N S を出力する。

## 【 0 0 2 0 】

（二）時刻  $t_3$  において、再びランダム信号 R S がローレベルからハイレベルとなる。カウンタ回路 1 は、ランダム信号 R S がハイレベルの状態が続く間、クロック信号 C S の立ち上がりエッジ検出毎に、カウント信号 C T S のレベルを交互に切り替える。

## 【 0 0 2 1 】

（ホ）時刻  $t_4$  において、ランダム信号 R S がハイレベルからローレベルとなる。ランダム信号 R S がローレベルとなると、インバータ 2 は、図 2（d）に示すように、ハイレベルとなるランダム反転信号 R S バーを出力する。ランダム反転信号 R S バーがハイレベルとなると、第 1 のラッチ回路 3 は、クロック入力端子 C K の立ち上がりエッジでカウンタ回路 1 から出力されるカウント信号 C T S をラッチし、図 2（e）に示すように、乱数信号 R N S を出力する。以後、同様にランダム信号 R S の立ち下がりエッジで乱数信号 R N S を出力する動作を繰り返す。

## 【 0 0 2 2 】

次に、乱数信号 R N S の出力が「0」または「1」である確率を図 3 を用いて説明する。ただし、ランダム信号 R S は  $y = F(s)$  の関数であると仮定して模式的に説明する。ランダム信号 R S を構成するランダムな矩形波のオン幅を T、

最小オン幅を  $T_{min}$ 、最大オン幅を  $T_{max}$  とする。また、最大オン幅  $T_{max}$  から最小オン幅  $T_{min}$  を引いたオン幅領域  $TZ$  から分解能設定クロック信号  $SC$  の周期で割った値を分割数  $N$  とする。オン幅領域  $TZ$  は、ランダムな矩形波の発生源となる抵抗、ダイオード等の素子が持つ周波数特性、矩形波を出力する回路の特性、及びフィルタ等の特性等によって決められる。この時、オン幅  $T$  のランダムな矩形波の分布関数を  $F(t)$  とすると、分割数  $N$  が偶数の時に乱数生成回路から「0」が出力される確率  $P_t(0)$  は、

【数 1】

$$P_t(0) = \int_{T_{min}}^{T_{min} + \frac{\Delta T}{N}} F(t) dt + \int_{T_{min} + \frac{2\Delta T}{N}}^{T_{min} + \frac{3\Delta T}{N}} F(t) dt + \dots + \int_{T_{min} + \frac{(N-2)\Delta T}{N}}^{T_{min} + \frac{(N-1)\Delta T}{N}} F(t) dt \dots (1)$$

で表される。

【0 0 2 3】

分割数  $N$  が偶数の時に乱数生成回路から 1 が出力される確率  $P_t(1)$  は、

【数 2】

$$P_t(1) = \int_{T_{min} + \frac{\Delta T}{N}}^{T_{min} + \frac{2\Delta T}{N}} F(t) dt + \int_{T_{min} + \frac{3\Delta T}{N}}^{T_{min} + \frac{4\Delta T}{N}} F(t) dt + \dots + \int_{T_{min} + \frac{(N-1)\Delta T}{N}}^{T_{max}} F(t) dt \dots (2)$$

で表される。

【0 0 2 4】

また、分割数  $N$  が奇数の時に乱数生成回路から 0 が出力される確率  $P_t(0)$  は、

【数 3】

$$P_t(0) = \int_{T_{min}}^{T_{min} + \frac{\Delta T}{N}} F(t) dt + \int_{T_{min} + \frac{2\Delta T}{N}}^{T_{min} + \frac{3\Delta T}{N}} F(t) dt + \dots + \int_{T_{min} + \frac{(N-1)\Delta T}{N}}^{T_{max}} F(t) dt \dots (3)$$

で表される。

【0 0 2 5】

分割数  $N$  が奇数の時に乱数生成回路から 1 が出力される確率  $P_t(1)$  は、

【数 4】

$$P_t(1) = \int_{T_{\min} + \frac{\Delta T}{N}}^{T_{\min} + \frac{2\Delta T}{N}} F(t) dt + \int_{T_{\min} + \frac{3\Delta T}{N}}^{T_{\min} + \frac{4\Delta T}{N}} F(t) dt + \dots + \int_{T_{\min} + \frac{(N-2)\Delta T}{N}}^{T_{\min} + \frac{(N-1)\Delta T}{N}} F(t) dt \dots (4)$$

で表される。

【0 0 2 6】

ここで、分割数Nが偶数となる場合の0と1が出る頻度の差は  $P_t(0) - P_t(1)$  で表される。これを計算すると、

【数 5】

$$P_t(0) - P_t(1) = \int_{T_{\min}}^{T_{\min} + \frac{\Delta T}{N}} \left\{ F(t) - F\left(t + \frac{\Delta T}{N}\right) + F\left(t + \frac{2\Delta T}{N}\right) - F\left(t + \frac{3\Delta T}{N}\right) + \dots - F\left(t + \frac{(N-2)\Delta T}{N}\right) + F\left(t + \frac{(N-1)\Delta T}{N}\right) \right\} dt \dots (5)$$

が求められる。

【0 0 2 7】

また、分割数Nが偶数となる場合の0と1が出る頻度の差は  $P_t(0) - P_t(1)$  で表され、これを計算すると

【数 6】

$$P_t(0) - P_t(1) = \int_{T_{\min}}^{T_{\min} + \frac{\Delta T}{N}} \left\{ F(t) - F\left(t + \frac{\Delta T}{N}\right) + F\left(t + \frac{2\Delta T}{N}\right) - F\left(t + \frac{3\Delta T}{N}\right) + \dots + F\left(t + \frac{(N-3)\Delta T}{N}\right) - F\left(t + \frac{(N-2)\Delta T}{N}\right) \right\} dt + \int_{T_{\min}}^{T_{\min} + \frac{\Delta T}{N}} F\left(t + \frac{(N-1)\Delta T}{N}\right) dt \dots (6)$$

が求められる。

【0 0 2 8】

式(5)及び式(6)より分割数Nが偶数、奇数に関わらず、分割数Nの値が大きい程「0」と「1」の出現する頻度の差は小さくなる。すなわち、クロック信号CSの周波数が高いほど、「0」と「1」の出現する頻度に偏りがなくなること示している。つまり、乱数を生成する場合は、使用する乱数の特性を考慮しクロック信号の周波数を選定する必要がある。

【0 0 2 9】

さらに、理想値 0.5 と 0 が出現する確率との差  $\delta(0)$  は、

【数 7】

$$\delta(0) = 0.5 - |(P_t(0) / (P_t(0) + P_t(1)))| \dots\dots\dots (7)$$

で表される。

【0 0 3 0】

また、理想値 0.5 と 1 が出現する確率との差  $\delta(1)$  は、

【数 8】

$$\delta(1) = 0.5 - |(P_t(0) / (P_t(0) + P_t(1)))| \dots\dots\dots (8)$$

で表される。

【0 0 3 1】

$\delta(0)$  と  $\delta(1)$  は、米国商務省が定める FIPS 140 [1] という規格検定によって利用分野により基準値が定められている。例えば、乱数生成回路を通信ネットワークのセキュリティに用いる場合は、 $\delta(0)$  または  $\delta(1)$  の値が 0.01375 以下でなければならない。すなわち、クロック信号 CK の周波数を基準値を満たすよう設定する必要がある。

【0 0 3 2】

また、ランダム信号 RS は、オン幅 T、オフ幅が一定でないので、振幅、周期、及び位相等の有限個のパラメータで特性を表現することができない。そこで、ランダム信号 RS を表現する方法としては、信号のパワーを一定の周波数帯域毎に分割し、各帯域毎のパワーを周波数の関数として表したパワースペクトルが用いられる。周期的信号波形のスペクトルは、基本周波数とその高調波成分から成り立っており、各成分の振幅の二乗の和で表すことができる。パワースペクトルは、時間関数  $x(t)$ 、パワースペクトル  $X(f)$  とすると、

【数 9】

$$X(f) = \int_0^{\infty} x(t)e^{-j2\pi ft} dt \dots\dots(9)$$

で表される。

## 【 0 0 3 3 】

乱数生成回路 1 0 a に入力されるランダム信号 R S は、図 4 に示すように、縦軸で示すパワースペクトルの信号強度が、横軸で示す周波数に対し反比例の関係にあるとする。この時、図 5 に示すように、ランダム信号 R S がオン幅 T である頻度の分布は、パワースペクトル特性で示す横軸方向を周波数から周期に変えた横軸方向に対称な曲線で示される。オン幅が T ( s ) である時の乱数生成回路の出力は、クロック信号 C S の周期  $T_{ck}$  毎に「 0 」または「 1 」を出力するかが決まる。クロック信号 C S の周期が小さい程、「 0 」と「 1 」が出現する確率はそれぞれ 0. 5 に近くなる。

## 【 0 0 3 4 】

図 6 で示す L 1 は、図 1 で示す乱数生成回路 1 0 a から出力される乱数信号 R N S のパワースペクトルを表す。また、L 2 は、 $1/f$  ノイズ源から生成されるランダム信号 R S のパワースペクトルを表す。ランダム信号 R S に対するパワースペクトルが周波数が高くなると減少してしまうのに対し、乱数信号 R N S のパワースペクトル L 1 は周波数特性に依存せず乱数信号 R N S を生成することができる。

## 【 0 0 3 5 】

更に、ランダム信号 R S を 8 ビットのシリアルデータとして入力した場合、前回のデータを縦軸で示す 0 ~ 2 5 5 に、次に取得されるデータを横軸に続けて 2 5 0 0 点プロットする。この時、乱数生成回路 1 0 a から出力される乱数信号 R N S は、図 7 ( a ) に示すように、ほぼ均一に分布する。これに対し、従来の乱数生成回路から出力される乱数は、図 7 ( b ) に示すように、バラツキが生じる。

## 【 0 0 3 6 】

本発明の第 1 の実施の形態に係る乱数生成回路 1 0 a によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「 0 」と「 1 」の出現する確率の調整を不要とすることが可能となる。

## 【 0 0 3 7 】

(第 2 の実施の形態)

本発明の第 2 の実施の形態に係る乱数生成回路 1 0 b は、図 8 に示すように、図 1 に示す乱数生成回路 1 0 a の第 1 のラッチ回路 3 の出力側に第 2 のラッチ回路 4 を 1 段追加している点で異なる。第 2 のラッチ回路 4 の入力端子 D は、第 1 のラッチ回路 3 の出力端子 Q に電氣的に接続される。また、第 2 のラッチ回路 4 の出力端子 Q は、乱数出力端子 5 3 に接続される。クロック入力端子 C K は乱数取得クロック入力端子 5 4 にそれぞれ接続されている。乱数取得クロック入力端子 5 4 は、周期が一定である乱数クロック取得信号を入力する端子である。他は第 1 の実施の形態と実質的に同様であるので、重複した記載を省略する。

## 【 0 0 3 8 】

次に、本発明の第 2 の実施の形態に係る乱数生成回路の動作を図 9 を用いて説明する。

## 【 0 0 3 9 】

(イ) 先ず、時刻  $t_1$  において、図 9 (a) に示すように、矩形波入力端子 5 1 に入力されるランダム信号 R S がローレベルからハイレベルとなる。

## 【 0 0 4 0 】

(ロ) 時刻  $t_1$  から  $t_2$  までの間、ランダム信号 R S がハイレベルの状態では、クロック信号 C S の立ち上がりエッジ検出毎に、カウンタ回路 1 の出力端子 Q から出力されるカウント信号 C T S のレベルは交互に切り替わる。

## 【 0 0 4 1 】

(ハ) 時刻  $t_2$  において、ランダム信号 R S がハイレベルからローレベルとなる。ランダム信号 R S がローレベルとなると、インバータ 2 は、図 9 (d) に示すように、ハイレベルとなるランダム反転信号 R S バーを出力する。ランダム反転信号 R S バーがハイレベルとなると、第 1 のラッチ回路 3 は、クロック入力端子 C K の立ち上がりエッジでカウンタ回路 1 から出力されるカウント信号 C T S をラッチし、図 9 (e) に示すように、第 1 の乱数信号 R N S 1 を出力する。

## 【 0 0 4 2 】

(ニ) 時刻  $t_3$  において、図 9 (f) に示すように、周期が一定である乱数取得クロック信号 R T S がローレベルからハイレベルとなる。第 2 のラッチ回路 4 は、乱数取得クロック信号 R T S の立ち上がりエッジで第 1 の乱数信号 R N S 1 を



ラッチし、図 9 (g) に示すように、第 2 の乱数信号 R N S 2 を出力する。以後、同様にランダム信号 R S の立ち下がりエッジで乱数信号 R N S を出力する動作を繰り返す。

#### 【 0 0 4 3 】

本発明の第 2 の実施の形態に係る乱数生成回路 1 0 b によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能となる。また、第 2 のラッチ回路 4 から出力される乱数信号 R N S を用いることにより一定時間間隔で乱数を取得することができる。

#### 【 0 0 4 4 】

##### (第 3 の実施の形態)

本発明の第 3 の実施の形態に係る乱数生成回路 1 0 c は、図 1 0 に示すように、図 1 に示す乱数生成回路 1 0 a のカウンタ回路 1 のカウントイネーブル端子 C E と矩形波入力端子 5 1 との間にパルスカウンタ 5 を備える点が異なる。パルスカウンタ 5 は、入力側を矩形波入力端子 5 1 に、出力側をカウンタ回路 1 のカウントイネーブル端子 C E にそれぞれ電氣的に接続する。他は第 1 の実施の形態と実質的に同様であるので、重複した記載を省略する。

#### 【 0 0 4 5 】

本発明の第 3 の実施の形態に係る乱数生成回路 1 0 c の動作を、図 1 1 を用いて説明する。

#### 【 0 0 4 6 】

(イ) 先ず、時刻  $t_1$  において、図 1 1 (a) に示す第 1 のランダム信号 R S 1 がローレベルからハイレベルとなる。パルスカウンタ 5 は、第 1 のランダム信号 R S 1 の立ち上がりエッジを検出すると、図 1 1 (b) に示すように、ハイレベルとなる第 2 のランダム信号 R S 2 を出力する。

#### 【 0 0 4 7 】

(ロ) 時刻  $t_1$  から  $t_2$  までの間、ランダム信号 R S がハイレベルの状態となる。この時、図 1 1 (d) に示すように、カウンタ回路 1 の出力端子 Q から出力されるカウント信号 C T S のレベルは、図 1 1 (c) に示すクロック信号 C S の

立ち上がりエッジ検出毎に交互に切り替わる。また、パルスカウンタ 5 は、ランダム信号 R S 1 の立ち上がりエッジをカウントする。ただし、パルスカウンタ 5 は例示的にカウント値が 2 になると出力を切り替えるとする。

## 【 0 0 4 8 】

(ハ) 時刻  $t_2$  において、パルスカウンタ 5 のカウント値が 2 になると、第 2 のランダム信号 R S 2 はハイレベルからローレベルとなる。第 2 のランダム信号 R S 2 がローレベルとなると、図 1 1 (d) に示すように、第 1 のラッチ回路 3 のクロック入力端子 C K はハイレベルとなる。第 1 のラッチ回路 3 は、クロック入力端子 C K の立ち上がりエッジでカウンタ回路 1 から出力されるカウント信号 C T S をラッチし、乱数出力端子 5 3 に乱数信号 R N S を出力する。以後、同様にランダム信号 R S の立ち下がりエッジで乱数信号 R N S を出力する動作を繰り返す。

## 【 0 0 4 9 】

本発明の第 3 の実施の形態に係る乱数生成回路 1 0 c によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能となる。また、ランダム信号の最小オン幅  $T_{min}$  がクロック信号 C S の周期  $T_{ck}$  に対し 2 倍以下であっても動作させることが可能となる。

## 【 0 0 5 0 】

## (第 4 の実施の形態)

本発明の第 4 の実施の形態に係る乱数生成回路 1 0 d は、図 1 2 に示すように、オン幅及びオフ幅が一定でないランダム信号 R S とクロック信号 C S を入力し、ランダム信号 R S 及びクロック信号 C S の論理積出力の変化に応じてハイレベルとローレベルを交互に切り替える分周信号 D R S を出力する分周回路 6 と、ランダム信号 R S の変化に応じて分周信号 D R S をラッチし乱数信号 R N S を出力する第 1 のラッチ回路 3 とを備える。

## 【 0 0 5 1 】

分周回路 6 は、第 1 の入力端子を矩形波入力端子 5 1 に、第 2 の入力端子をクロック入力端子 5 2 にそれぞれ接続されるアンド回路 2 0 と、アンド回路 2 0 の

出力端子をクロック入力端子に接続する分周ラッチ回路 2 1 と、分周ラッチ回路 2 1 の出力端子 Q と入力端子 D との間に接続されたインバータ 2 2 とを備える。

【 0 0 5 2 】

本発明の第 4 の実施の形態に係る乱数生成回路 1 0 d の動作を図 1 3 を用いて説明する。

【 0 0 5 3 】

(イ) 先ず、図 1 3 ( a ) に示すように、時刻 t 1 において、矩形波入力端子 5 1 に入力されるランダム信号 R S がローレベルからハイレベルとなる。

【 0 0 5 4 】

(ロ) 時刻 t 1 から t 2 までの間、ランダム信号 R S がハイレベルの状態では、図 1 3 ( c ) に示すように、アンド回路 2 0 の出力端子から図 1 3 ( b ) に示すクロック信号 C S がそのまま出力される。この時、図 1 3 ( d ) に示すように、クロック信号 C S の立ち上がりエッジ検出毎に分周ラッチ回路 2 1 の出力端子 Q から出力される分周信号 D R S のレベルは交互に切り替わる。

【 0 0 5 5 】

(ハ) 時刻 t 2 において、ランダム信号 R S がハイレベルからローレベルとなると、図 1 3 ( e ) に示すように、第 1 のラッチ回路 3 のクロック入力端子 C K はハイレベルとなる。クロック入力端子 C K がハイレベルとなると、第 1 のラッチ回路 3 は分周信号 D R S をラッチし、図 1 3 ( f ) に示すように、乱数出力端子 5 3 から乱数信号 R N S を出力する。以後、同様にランダム信号 R S の立ち上がりエッジで乱数信号 R N S を出力する動作を繰り返す。

【 0 0 5 6 】

本発明の第 4 の実施の形態に係る乱数生成回路 1 0 d によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「 0 」と「 1 」の出現する確率の調整を不要とすることが可能となる。

【 0 0 5 7 】

(第 5 の実施の形態)

本発明の第 5 の実施の形態に係る乱数生成回路 1 0 e は、図 1 4 に示すように、図 1 2 で示す乱数生成回路 1 0 d が分周ラッチ回路としてラッチ回路 2 1 ( D

型フリップフロップ)を用いているのに対し、ラッチ回路23(J-K型フリップフロップ)を用いる点で異なる。また、第1のラッチ回路3(D型フリップフロップ)もを用いているのに対し、ラッチ回路7(J-K型フリップフロップ)を用いる点で異なる。他は第1の実施の形態と実質的に同様であるので、重複した記載を省略する。

## 【0058】

本発明の第5の実施の形態に係る乱数生成回路10eの動作を、図15を用いて説明する。

## 【0059】

(イ) 先ず、時刻 $t_1$ において、図15(a)に示すように、ランダム信号RSがローレベルからハイレベルとなる。

## 【0060】

(ロ) 時刻 $t_1$ から $t_2$ までの間、ランダム信号RSがハイレベルの状態では、図15(c)に示すように、アンド回路20の出力端子から図15(b)に示すクロック信号CSがそのまま出力される。この時、図15(d)に示すように、クロック信号CSの立ち上がりエッジ検出毎に分周ラッチ回路23の出力端子Qから出力される分周信号DRSのレベルは交互に切り替わる。

## 【0061】

(ハ) 時刻 $t_2$ において、ランダム信号RSがハイレベルからローレベルとなると、図15(f)に示すように、ラッチ回路7のクロック入力端子CKはハイレベルとなる。この時、ラッチ回路7の第1の入力端子Jには、図15(d)に示すように、分周信号DRSが入力される。また、ラッチ回路7の第2の入力端子Kには、図15(e)に示すように、分周信号DRSを反転した分周反転信号DRSバーが入力される。ラッチ回路7は、ランダム信号RSを反転したランダム反転信号RSバーの立ち上がりエッジで分周信号DRSをラッチし、図15(g)に示すように、乱数信号RNSを出力する。乱数信号RNSは乱数信号出力端子53から出力される。以後、同様にランダム信号RSの立ち下がりエッジで乱数信号RNSを出力する動作を繰り返す。

## 【0062】

本発明の第5の実施の形態に係る乱数生成回路10eによれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能となる。

【0063】

(その他の実施の形態)

上記のように、本発明は第1～第5の実施の形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなろう。

【0064】

既に述べた第4～第5の実施の形態に係る乱数生成回路10d、10eについては、第2の実施の形態で示すような第2のラッチ回路を更に設けることが可能である。また、乱数生成回路10d、10eは、第3の実施の形態で示すように、ラッチ回路の出力に、更にパルスカウンタを設けることも可能である。

【0065】

既に述べた第1～第5の実施の形態に係る乱数生成回路10a、10b、10c、10d、10eで用いられるクロック信号CSの周期は、ランダム信号RSの最小オン幅 $T_{min}$ の2倍以上であることが望ましい。クロック信号CSの周期Tを最小オン幅 $T_{min}$ に対して大きく設定するほどランダム信号RSのパワースペクトルの差異による影響を抑えることができる。

【0066】

このように、本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

【0067】

【発明の効果】

本発明によれば、複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能な乱数生成回路を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態に係る乱数生成回路を説明する図である。

【図 2】

本発明の第 1 の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図 3】

本発明の第 1 の実施の形態に係る乱数生成回路に入力するランダム信号を説明する図である。

【図 4】

本発明の第 1 の実施の形態に係るランダム信号のパワースペクトルを模式的に説明する図である。

【図 5】

本発明の第 1 の実施の形態に係る乱数生成回路により生成される乱数信号を説明する図である。

【図 6】

本発明の第 1 の実施の形態に係る乱数生成回路により生成される乱数信号のパワースペクトルを説明する図である。

【図 7】

図 7 ( a ) は、本発明の第 1 の実施の形態に係る乱数生成回路により生成される乱数信号の周期性を説明する図である。

図 7 ( b ) は、従来の乱数生成回路により生成される乱数信号の周期性を説明する図である。

【図 8】

本発明の第 2 の実施の形態に係る乱数生成回路を説明する図である。

【図 9】

本発明の第 2 の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図 1 0】

本発明の第 3 の実施の形態に係る乱数生成回路を説明する図である。

【図 1 1】

本発明の第 3 の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図 1 2】

本発明の第 4 の実施の形態に係る乱数生成回路を説明する図である。

【図 1 3】

本発明の第 4 の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図 1 4】

本発明の第 5 の実施の形態に係る乱数生成回路を説明する図である。

【図 1 5】

本発明の第 5 の実施の形態に係る乱数生成回路の動作タイミングチャートである。

【図 1 6】

従来の乱数生成回路について説明する図である。

【符号の説明】

- 1 … カウンタ回路
- 2, 2 2 … インバータ
- 3 … 第 1 のラッチ回路
- 4 … 第 2 のラッチ回路
- 5 … パルスカウンタ
- 6 … 分周回路
- 1 0 a, 1 0 b, 1 0 c, 1 0 d, 1 0 e … 乱数生成回路
- 2 0 … アンド回路
- 2 1 … 分周ラッチ回路
- 5 1 … 矩形波入力端子
- 5 2 … クロック入力端子
- 5 3 … 乱数出力端子

5 4 …乱数取得クロック入力端子

2 0 1, 2 0 2 …雑音発生回路

2 0 3 …差動回路

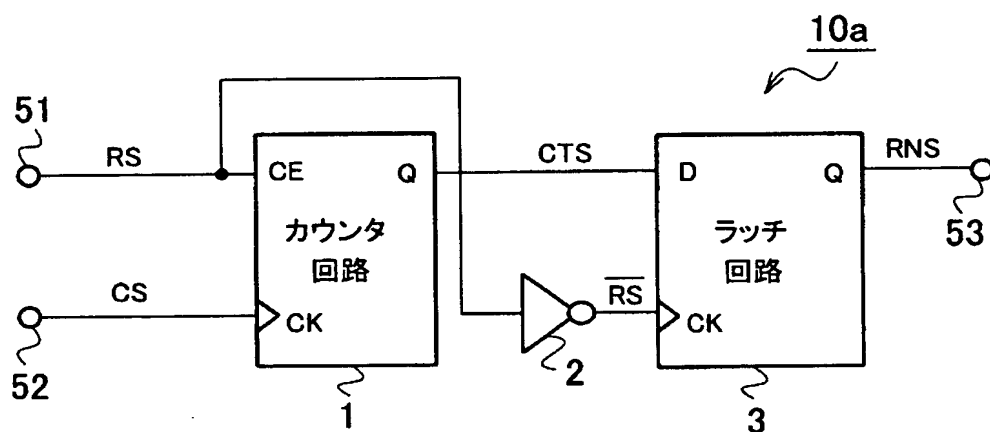
2 0 4 …D変換回路

2 0 5 …演算回路

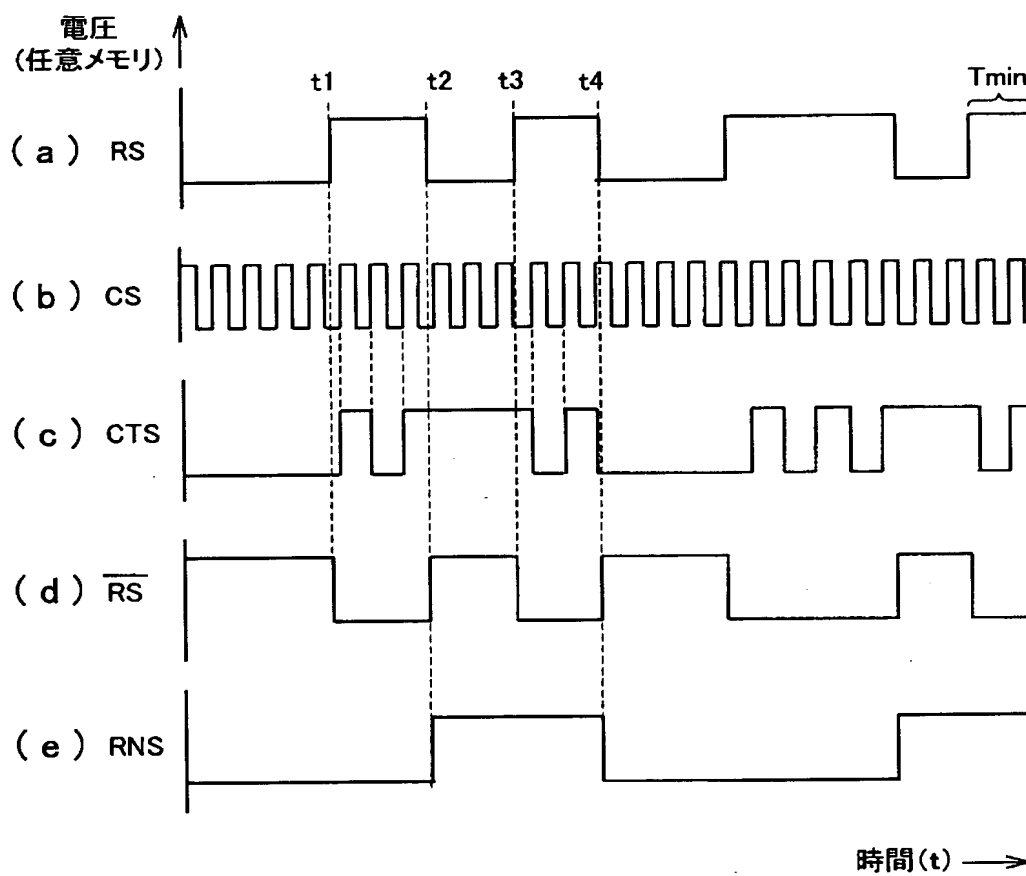


【書類名】 図面

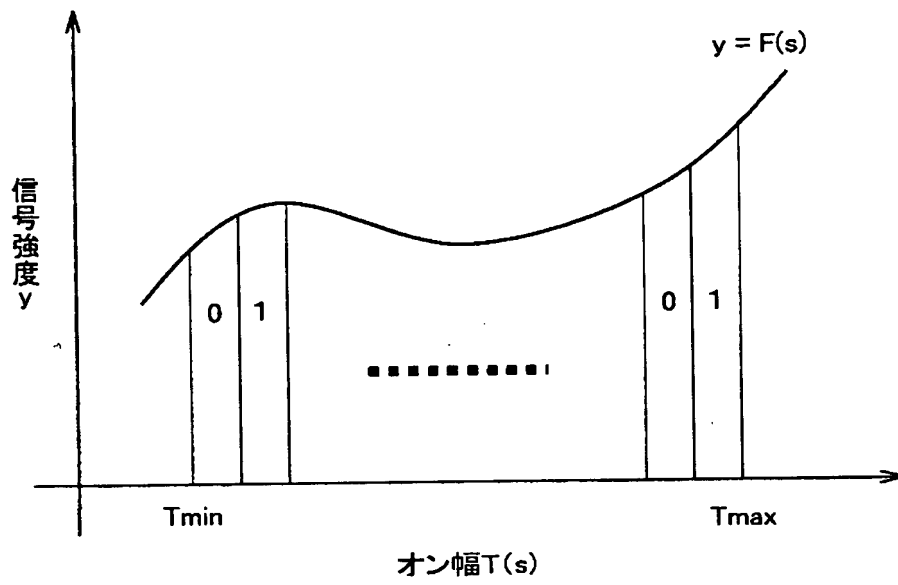
【図 1】



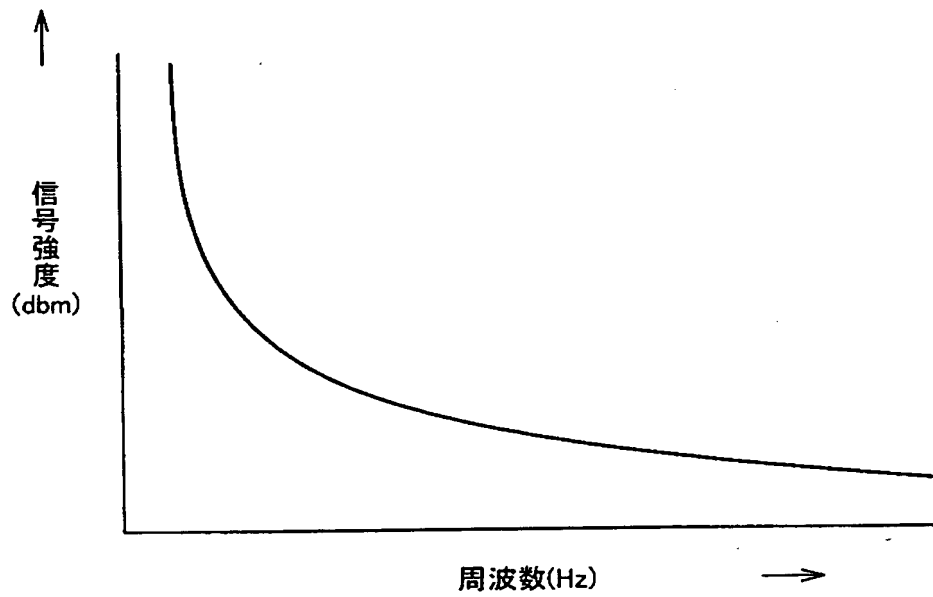
【図 2】



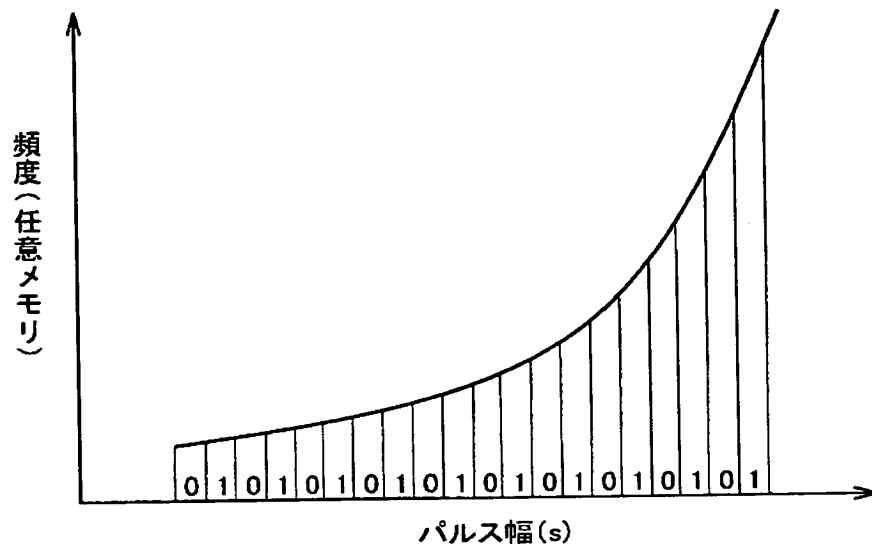
【図 3】



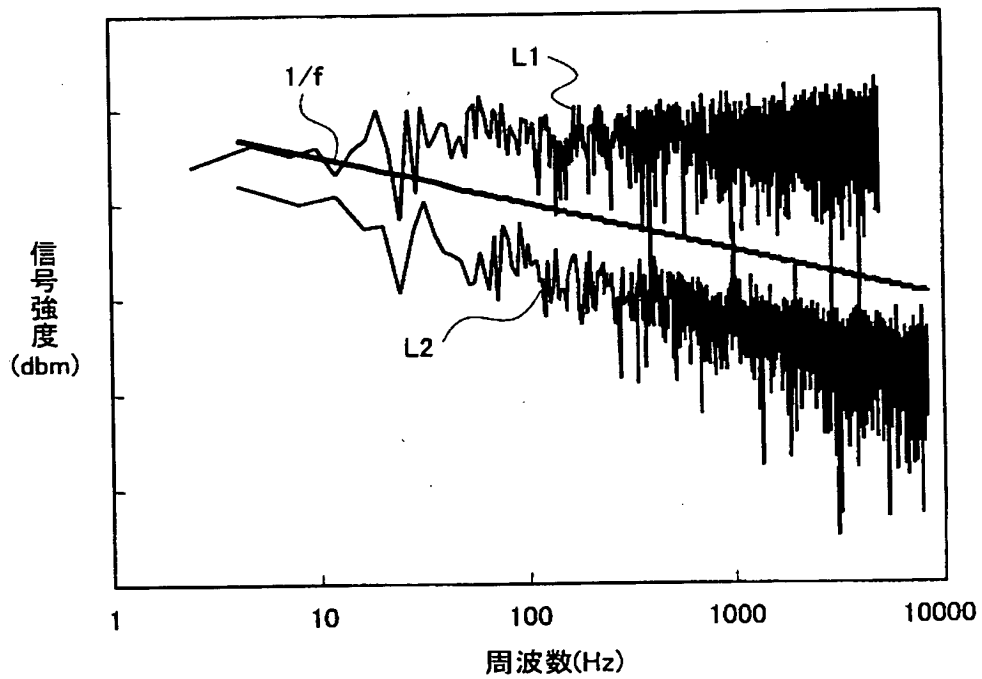
【図 4】



【図 5】

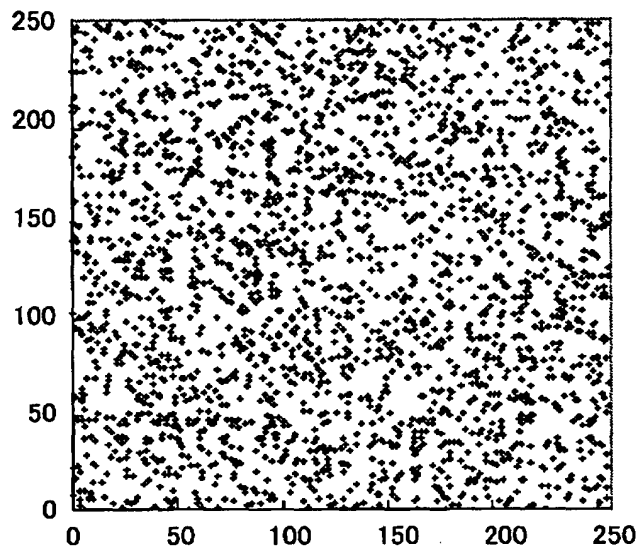


【図 6】

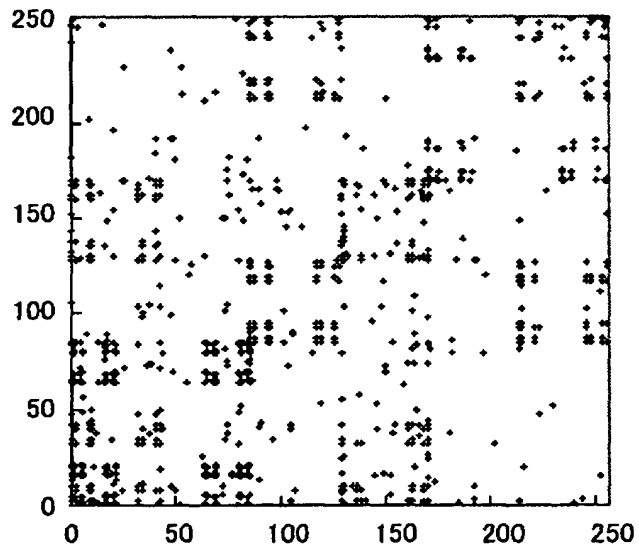


【図 7】

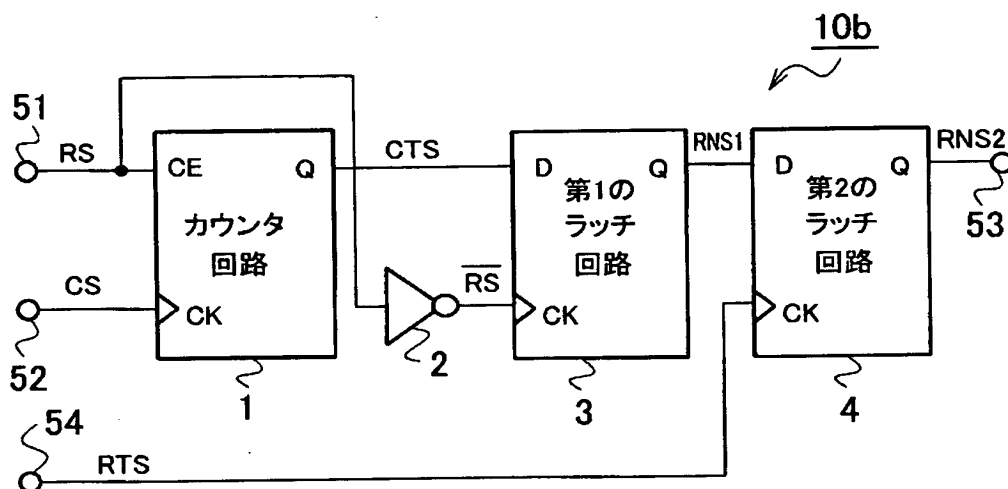
( a )



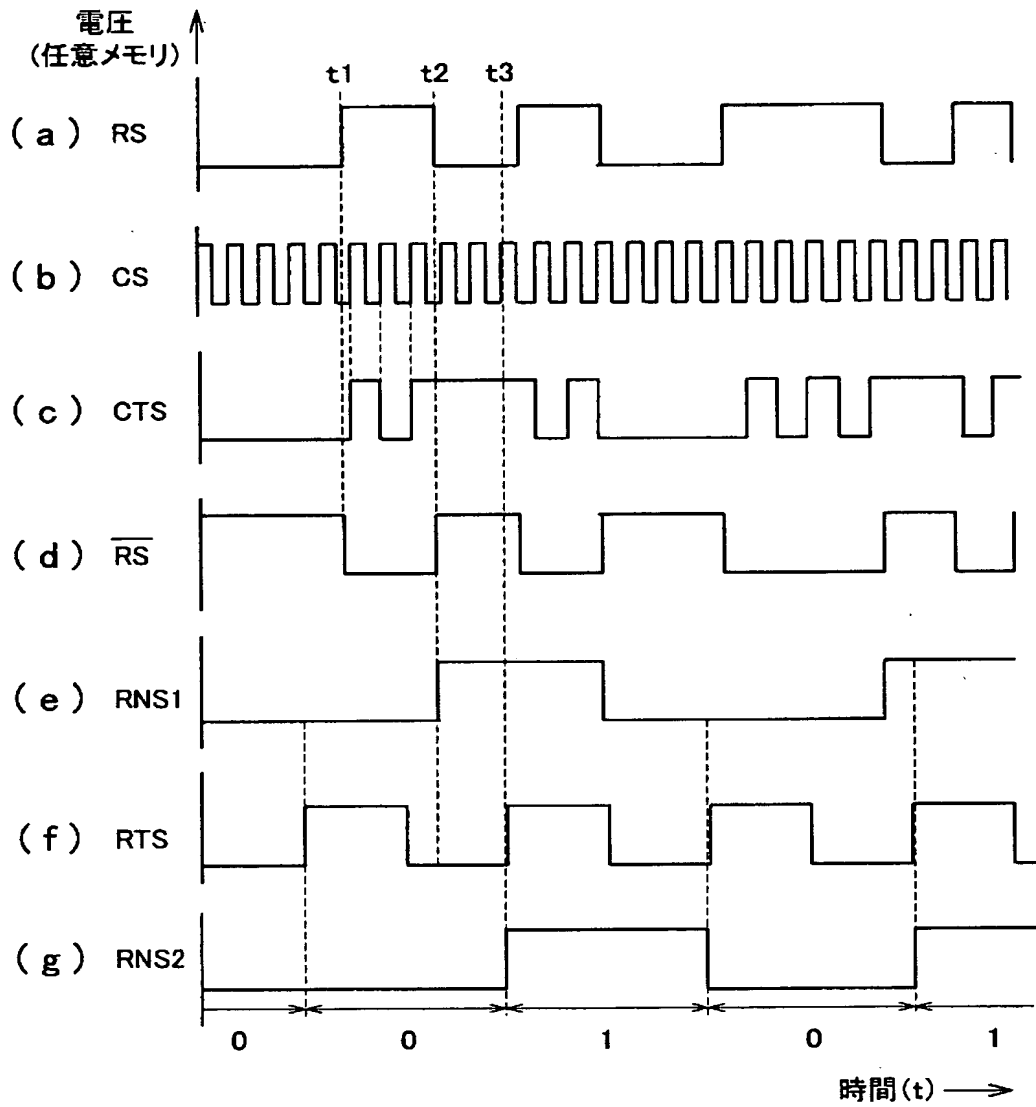
( b )



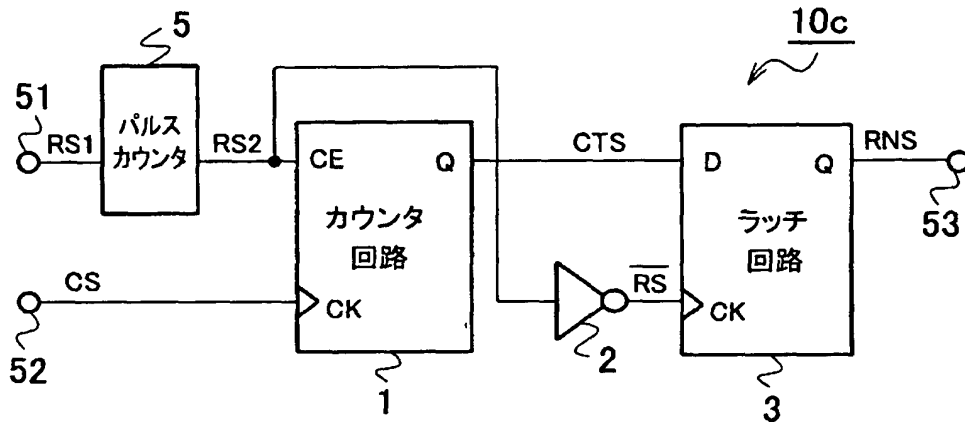
【図 8】



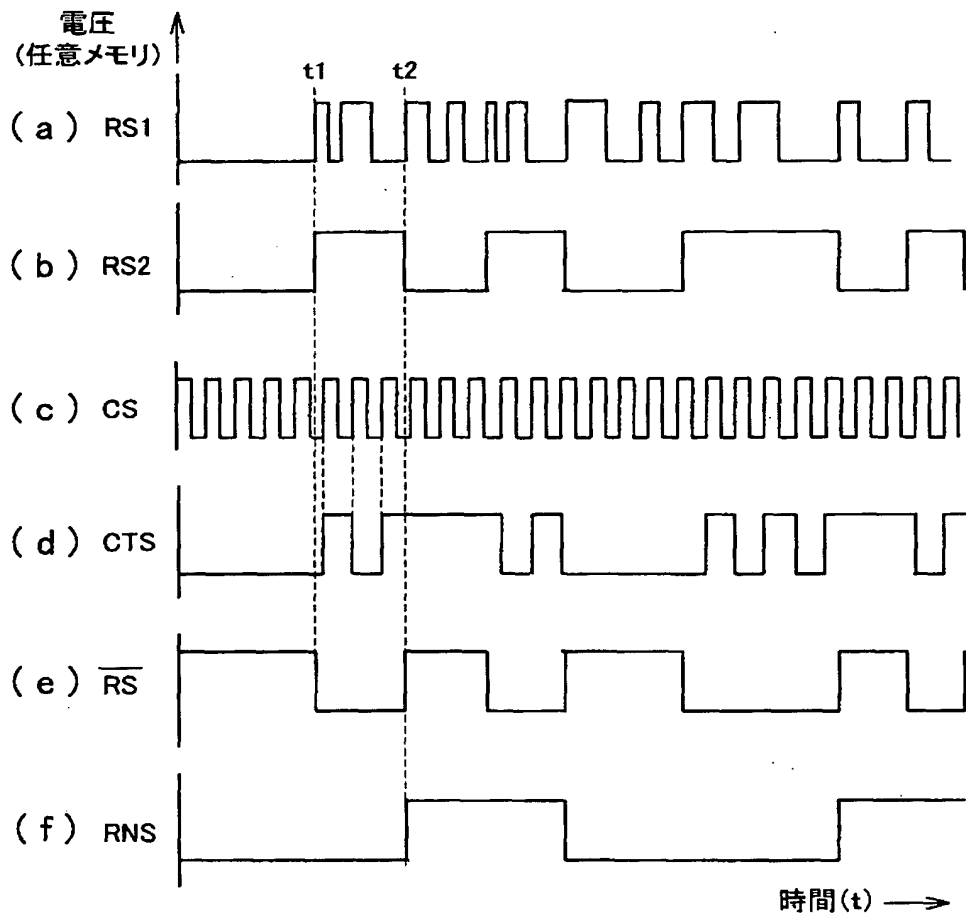
【図 9】



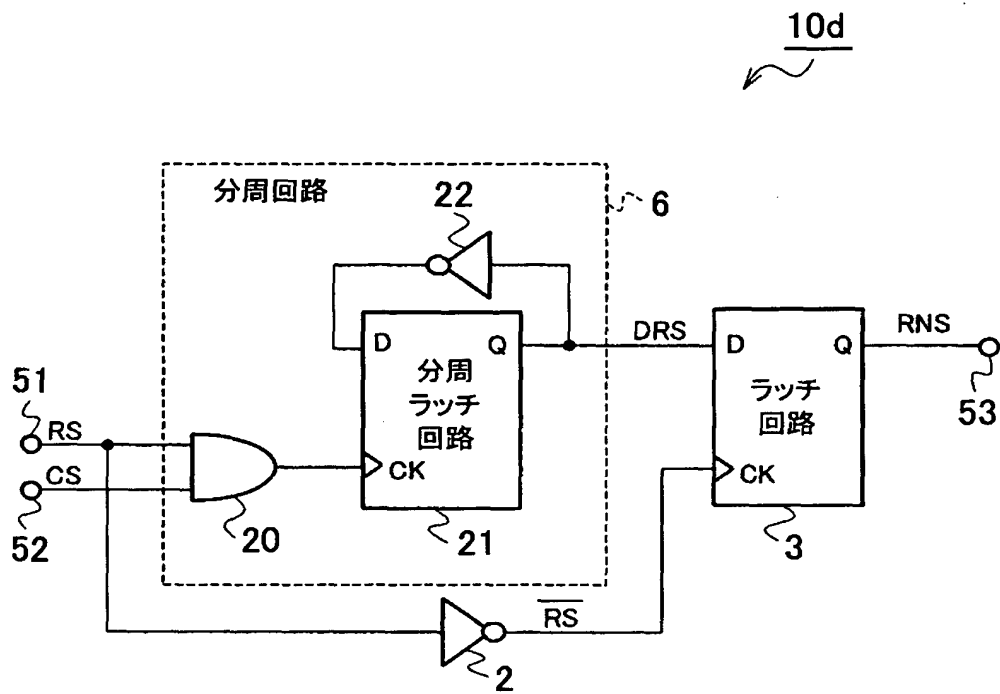
【図 1 0】



【図 1 1】

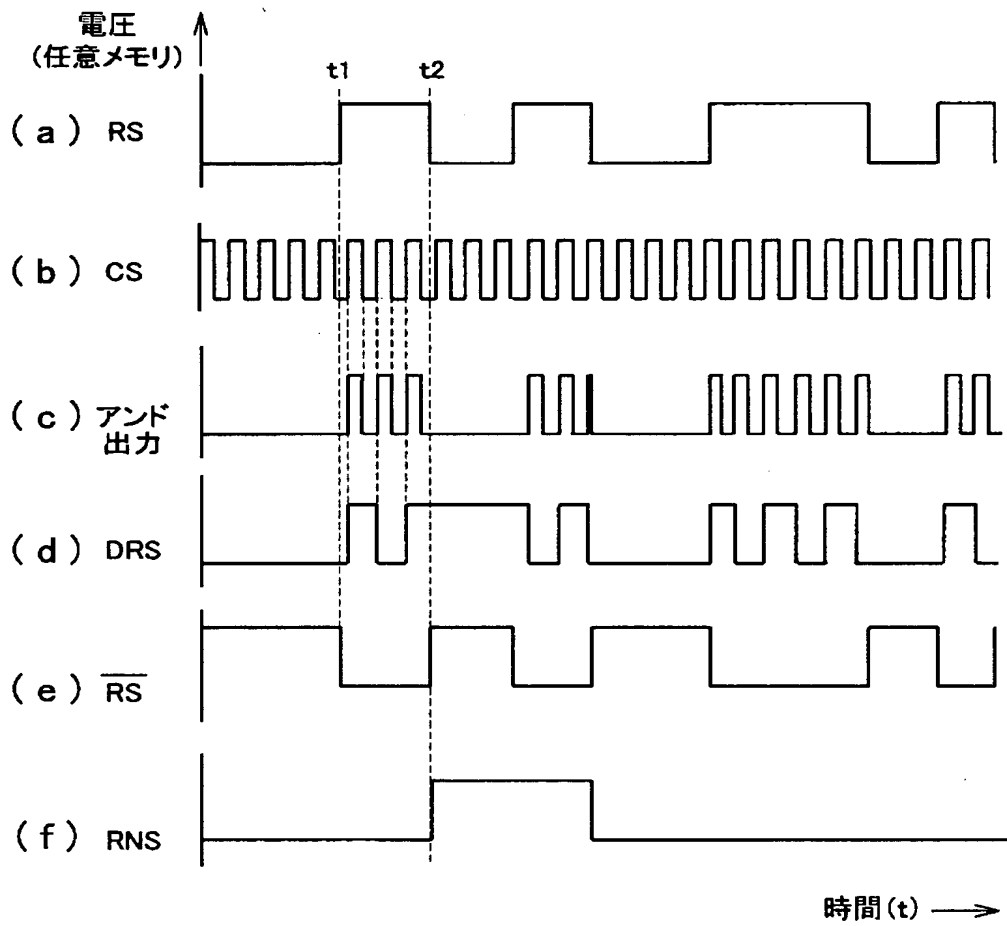


【図 1 2】

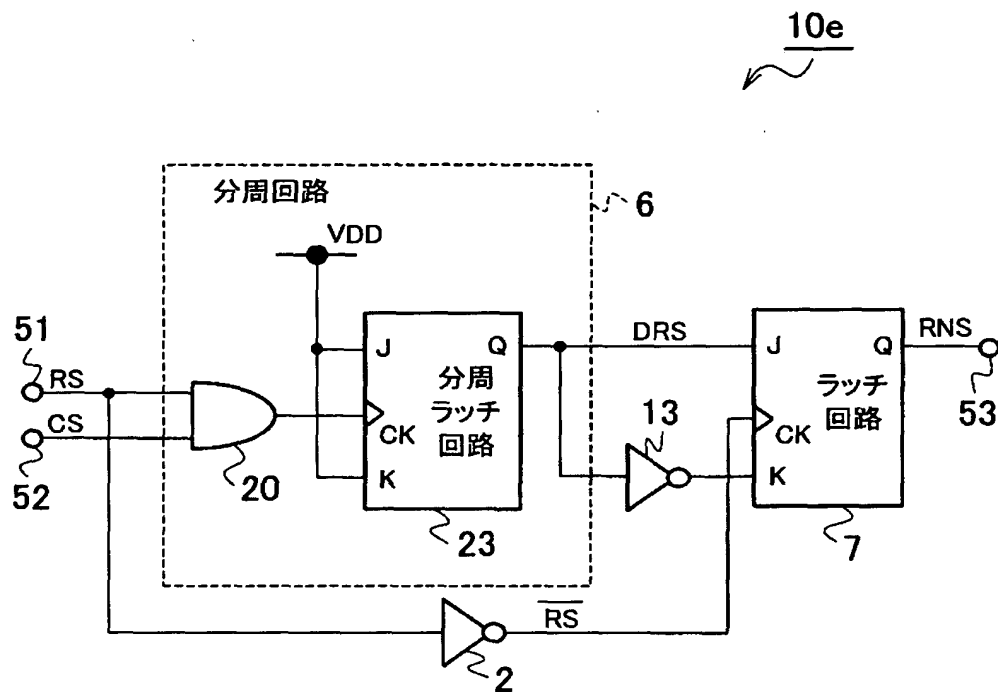




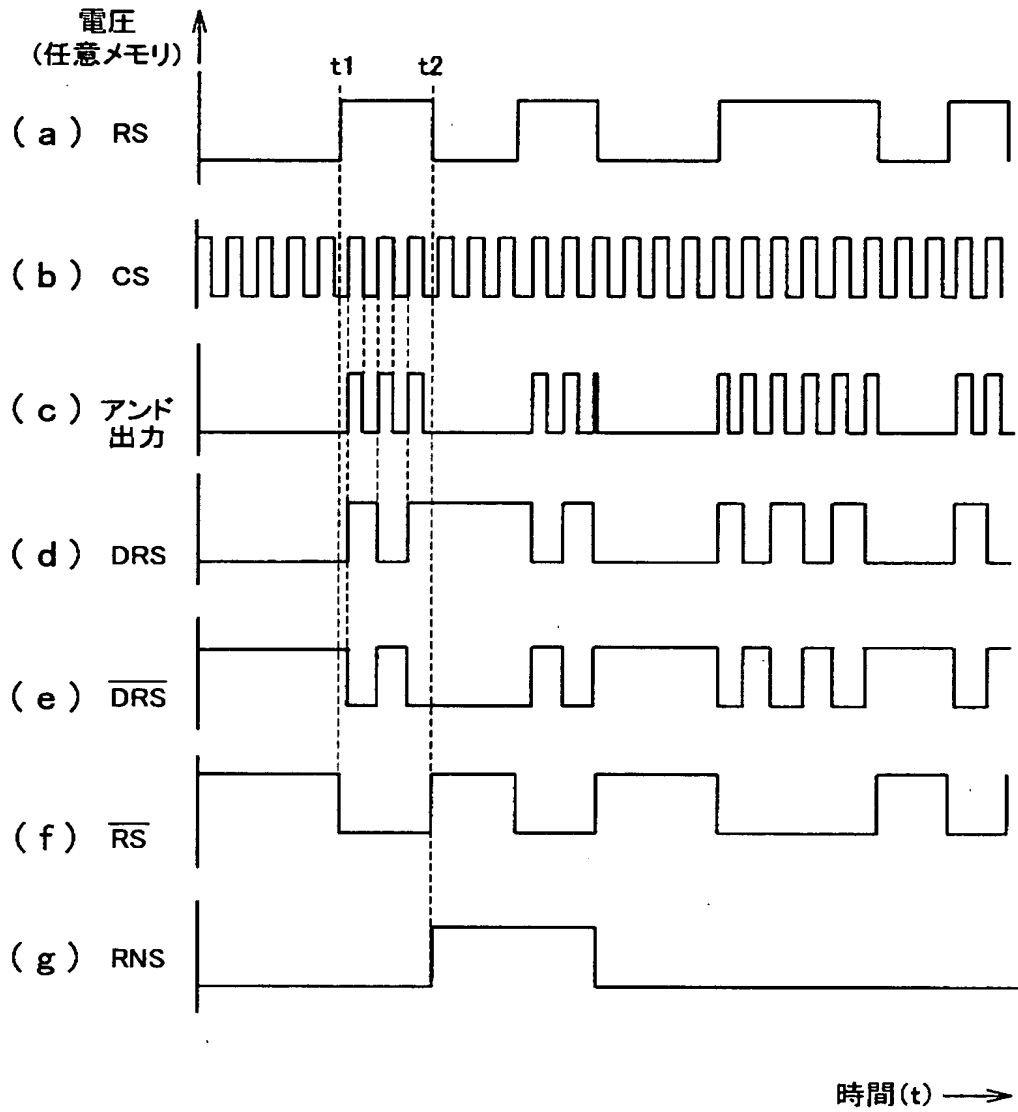
【図 1 3】



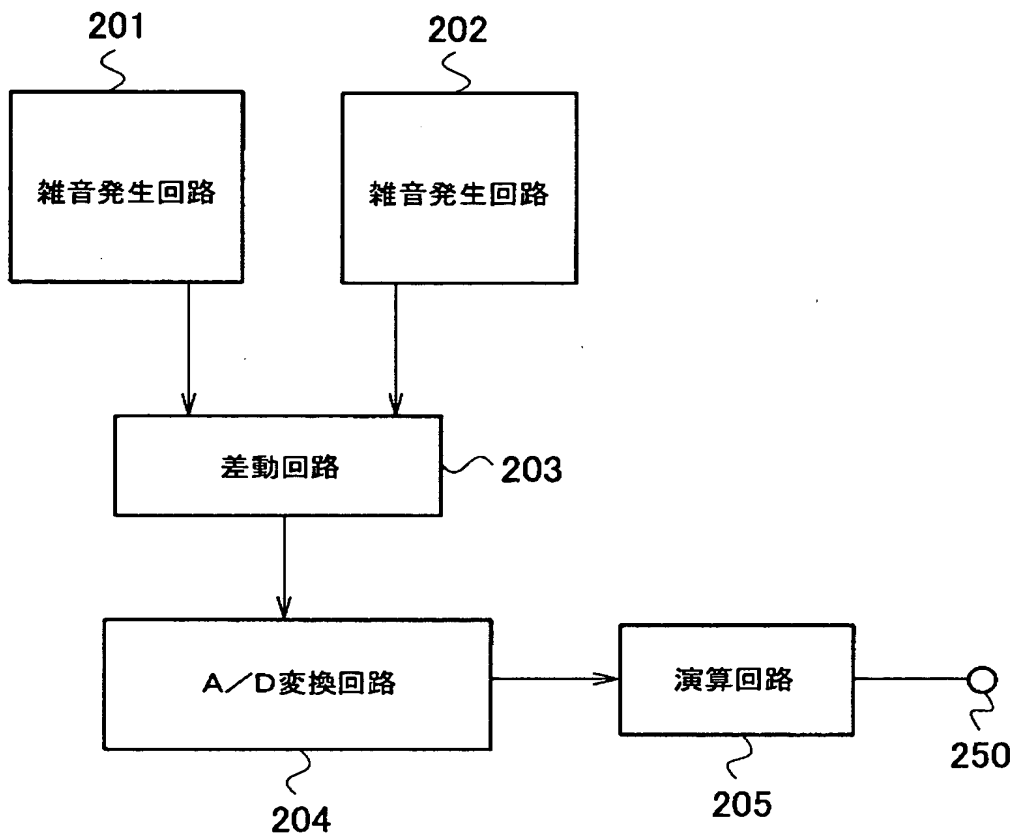
【図 1 4】



【図 1 5】



【図 1 6】



【書類名】            要約書

【要約】

【課題】    複数の雑音発生回路を用いず、小型化が可能であり、周波数特性に依存しない乱数を生成し、「0」と「1」の出現する確率の調整を不要とすることが可能な乱数生成回路を得る。

【解決手段】    ランダム信号 R S とクロック信号 C S を入力し、ランダム信号 R S の変化に応じてクロック信号 C S のカウント値を出力するカウンタ回路 1 と、ランダム信号 R S の変化に応じてカウント値をラッチし乱数信号 R N S を出力する第 1 のラッチ回路 3 とを備える。

【選択図】            図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	2001年 7月 2日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目1番1号
氏 名	株式会社東芝